IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 3:18-cr-00118-001-HEH
	)	
CHRISTOPHER BRANNAN	)	
	)	
Defendant.	)	
	)	

UNITED STATES' POSITION WITH RESPECT TO SENTENCING FACTORS

The United States of America, by and through its attorneys, G. Zachary Terwilliger, United States Attorney for the Eastern District of Virginia, and Brian R. Hood, Assistant United States Attorney, hereby submits its position with respect to the sentencing factors for the defendant, CHRISTOPHER BRANNAN. The United States has reviewed the Presentence Investigation Report (PSR), and has no objections to that Report. The PSR calls for a guideline range of 10-16 months' incarceration on Count One, which charged defendant with unauthorized access to a computer to obtain information from a protected computer, and 24 months' consecutive on Count Two, which charged the defendant with aggravated identity theft. For the reasons set below, the Government recommends that the Court impose a sentence at the low end of the guideline range of 34 months' incarceration.

I. CASE SUMMARY

The Statement of Facts (SOF) accompanying the defendant's guilty plea and the PSR set forth the essential details of the defendant's offense. Between August 27, 2013, and October 2, 2014, the defendant, Christopher Brannan, accessed without authorization hundreds of email and social media accounts belonging to celebrities and noncelebrities that were hosted by Yahoo!, Apple Inc. ("Apple"), Facebook, and other internet service providers. He did so in order to view

their contents and, in many cases, extract photographs and other private information, and share them with others. (SOF ¶ 1; PSR ¶¶ 11-13.)

Defendant carried out his hacking scheme through various methods. Sometimes, he would identify usernames and passwords through simple online research. (SOF ¶ 2.) Sometimes, defendant would use a phishing scheme whereby he would use fraudulent email accounts from Apple misrepresenting to the victims that the emails had come from Apple in order to obtain username and password information for the victims' internet accounts. Because of the victims' belief that the email had come from Apple, the victims would provide their usernames and passwords. (SOF ¶ 2; PSR ¶ 14.)

Regardless of his means of access, once inside the accounts, defendant would search the content of the victims' email accounts, and obtain personal information, such as sensitive and private photographs and videos, including nude photographs. In the case of at least eighteen Apple iCloud accounts, he used specialized software to extract the complete contents of the victim's iCloud account and download it to his computer, which contents included sensitive and private photographs and videos. (SOF ¶¶ 2-3; PSR ¶ 16.) Defendant also either attempted to access or successfully accessed the email account of his sister-in-law, who was then a minor, as well as the internet accounts of numerous current and former teachers and students at the high school where defendant worked. (SOF ¶ 3.)

Defendant would often trade the usernames and passwords, as well as the materials he stole from the victims, with other individuals. (SOF ¶ 4.) On at least one occasion, defendant obtained the assistance of another individual to hack into a victim's email account. (*Id.*)

II. SENTENCING ANALYSIS SINCE *UNITED STATES V. BOOKER*

In *United States v. Booker*, 543 U.S. 220 (2005), the Supreme Court held that mandatory imposition of sentences derived from the Federal Sentencing Guidelines violated a defendant's Sixth Amendment right to a jury trial. The Court further held that district courts, while not bound to apply the Guidelines, must consult them and take them into account when sentencing, as well as the factors listed in 18 U.S.C. §3553. *Id.* at 265.

In *United States v. Moreland*, 437 F.3d 424 (4th Cir. 2006), the Fourth Circuit described an analytical approach district courts must adhere to in determining an appropriate sentence. The *Moreland* approach requires that a district court: 1) correctly determine the applicable guideline range; 2) assess whether the guideline range satisfies the § 3553(a) factors; 3) consider any appropriate departures under the Guidelines and the case law that might also be necessary; and, finally, 4) consider, and explain, a variance to a non-guideline sentence if such a variance is still required to satisfy the factors in § 3553(a). *Moreland*, 437 F.3d at 432.

Title 18, United States Code, Section 3553(a) mandates that a sentencing court impose a sentence that is sufficient, but not greater than necessary, to comply with the purposes set forth in § 3553(a)(2). In determining such a sentence, § 3553 requires that the Court consider the following factors:

> (1) the nature and circumstances of the offense, and the history and characteristics of the defendant;
>
> (2) the need for the sentence imposed—
>
> > (A) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense;
> >
> > (B) to afford adequate deterrence to criminal conduct;
> >
> > (C) to protect the public from further crimes by the defendant; and
> >
> > (D) to provide the defendant with needed educational or vocational

> training; medical care, or other correctional treatment in the most effective manner.

III. PRESENTENCE REPORT'S GUIDELINE ANALYSIS

The applicable guideline section for Count One, unauthorized access to a computer to obtain information from a protected computer (18 U.S.C. § 1030(a)(2)(C), (c)(2)(B)(ii), (iii)), is USSG § 2B1.1. Pursuant to § 2B1.1(a)(1), defendant's base offense level is 6. Defendant receives two a 2-level enhancement for 10 or more victims, under § 2B1.1(b)(2)(A), and, because defendant engaged in sophisticated means, defendant's offense level is increased to 12 under § 2B1.1(b)(10)(C) (which is effectively a 4-level enhancement). Finally, defendant receives another enhancement for being convicted of an offense under 18 U.S.C. § 1030 that involved the intent to obtain personal information under § 2B1.1(b)(17)(A). With a 2-level reduction for Acceptance of Responsibility under USSG §3E1.1, the defendant's Total Offense Level is 12. The defendant has 0 criminal history points, and thus with a Criminal History Category of I his guideline range for Count One is 10-16 months.

The applicable guideline section for aggravated identity theft as charged in Count Two is § 2B1.6, which calls for imposition of the statutory mandatory minimum sentence of 24 months' incarceration. BRANNAN's total guideline range is thus 34-40 months.

IV. FACTORS UNDER 18 U.S.C. § 3553(A)(1)

A. Nature and Circumstances of the Offense

Defendant's offense was a serious one. He illegally hacked into his victims' online accounts, invaded their privacy, and stole their personal information, including private and intimate photos and videos. This was anything but impulsive; rather, he engaged in this conduct thousands of times to gain access to hundreds of accounts over the course of 13 months.

Although defendant engaged in the offense by hiding behind a computer, his actions essentially amounted to breaking into hundreds of homes, searching through his victims' closets and drawers, and stealing their personal belongings. The fact that the items he stole were private photographs and videos, as opposed to other tangible items, makes no difference. In many cases, these were nude and intimate photos that no one else was meant to see. Notably, defendant either attempted to access, or successfully accessed, the account of his underage sister-in-law.[1] He also targeted former students and teachers at the high school where he worked.

What makes matters worse is that defendant traded the photographs – and stolen login credentials – with others. Once he disseminated them, there was no stopping their spread and further circulation. Defendant has apologized and expressed remorse for his actions, but he cannot put the proverbial genie back in the bottle. The information and nude photographs he disseminated are now forever in circulation, and each time someone else views any one of those private photographs, the victim is re-victimized all over again. Such conduct is serious and merits a substantial sentence of 34 months, as the parties have agreed to recommend.

B. History and Characteristics of the Defendant

1. Criminal History

Defendant has no known history of prior criminal convictions, so he receives no criminal history points and is thus for guideline purposes is a Criminal History Category I.

2. Personal History and Characteristics

Based on interviews of defendant and his mother, as well as review of records, we know that defendant was raised between the two homes of his parents, who divorced when he was a toddler. (PSR ¶ 44.) He appears to have had a stable upbringing without the influence of drugs

[1] To be clear, law enforcement found no evidence of child pornography on defendant's computer.

or alcohol, and surrounded by much family who loved him and showed him attention by attending his school and extra-curricular activities. (PSR ¶ 45.) After attending college, defendant got married, but he is now divorced. (PSR ¶ 47.)

V. FACTORS UNDER 18 U.S.C. § 3553(A)(2)

A. Seriousness of the Offense

As discussed above, hacking of online accounts, stealing private information, and sharing it with others, is a serious offense. Defendant hacked and attempted to hack hundreds of accounts on thousands of occasions, cataloguing what he would steal on his computer, and renaming thousands of files. In at least eighteen instances, he downloaded the complete contents of victims' iCloud accounts. This serious criminal conduct warrants a serious sentence of 34 months.

B. Need to Deter Future Criminal Conduct

Although defendant has no criminal history, as noted above, defendant's conduct occurred thousands of times over the course of 13 months. Thus, it was most certainly not impulsive, and was instead calculated and thorough. Defendant's targeting of his underage sister-in-law is particularly troubling. A strong sentence in this case of 34 months should help provide a measure of deterrence, not just to the defendant himself but also to others who would seek to engage in such criminal conduct.

C. Need to Protect the Public from the Defendant's Future Criminal Conduct

A sentence of 34 months' incarceration would similarly provide appropriate protection to the public from the defendant's future criminal conduct for the period of time he is incarcerated.

D. Need to Provide Treatment to Defendant

The United States is not aware that the defendant has any medical, psychological or substance abuse issues that require treatment.

VI. CONCLUSION

For all of the reasons set forth above, the United States asks the court to impose a sentence at the bottom of the applicable guideline range of 34 months' incarceration.

Respectfully submitted,

G. ZACHARY TERWILLIGER
UNITED STATES ATTORNEY

By: */s/ Brian R. Hood*

Assistant United States Attorney
United States Attorney's Office
919 East Main Street, Suite 1900
Richmond, VA 23219
Telephone: (804) 819-5400
Email: brian.hood@usdoj.gov

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on **February 21, 2019**, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of such filing (NEF) to all parties of record.

Respectfully submitted,

G. ZACHARY TERWILLIGER
UNITED STATES ATTORNEY

By: */s/ Brian R. Hood*
Assistant United States Attorney
United States Attorney's Office
919 East Main Street, Suite 1900
Richmond, VA 23219
Telephone: (804) 819-5400
Email: brian.hood@usdoj.gov